CobiT: Visão Geral e domínio Monitorar e Avaliar

Daniel Baptista Dias
Ernando Eduardo da Silva
Leandro Kaoru Sakamoto
Paolo Victor Leite e Posso

CobiT – O que é ?

- Um framework contendo boas práticas para a auditoria e governança da tecnologia da informação em organizações.

- Visa atender:
  - Requisitos de negócios;
  - Requisitos regulatórios (como a Sarbanes-Oxley e a Basiléia II);
  - Gerenciamento de riscos
  - Etc…

CobiT - Bases

- O CobiT é baseado em 4 pilares:

Foco em negócios

Orientação a processos

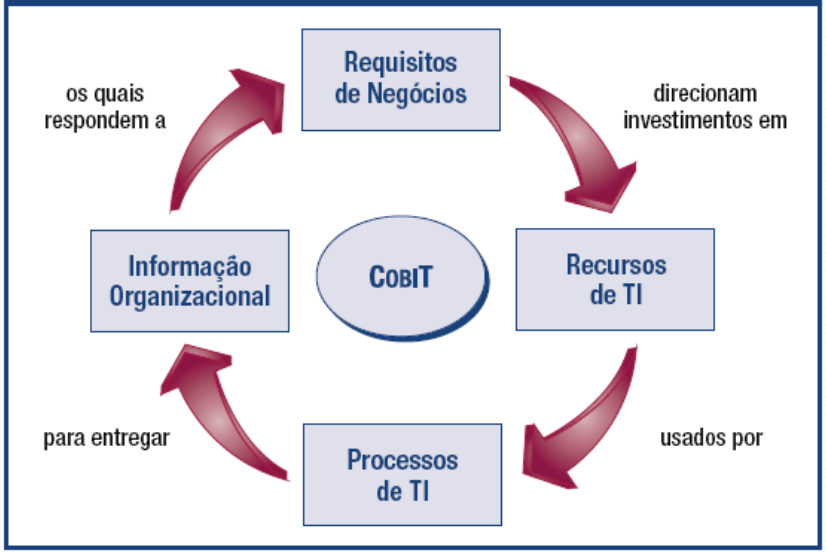
Base em controles

Orientação por medições

CobiT – Foco em negócios

- Para se focar em negócios o CobiT baseia-se nos seguintes princípios:
  - Prover a informação de que a organização precisa para atingir os seus objetivos, as necessidades para investir, gerenciar e controlar os recursos de TI usando um conjunto estruturado de processos para prover os serviços que disponibilizam as informações necessárias para a organização.

Figura 5 - Princípios Básicos do CobiT



CobiT – Foco em negócios

- Para assegurar o alinhamento com os objetivos de negócio, definimos **critérios de informação**:
  - Efetividade: lidar com informações pertinentes ao negócio entregando-as de maneira correta, consistente e utilizável
  - Eficiência: entrega da informação através do melhor uso dos recursos
  - Confidencialidade: proteção das informações confidenciais para evitar divulgação indevida

CobiT – Foco em negócios

- **Critérios da Informação:**
  - Integridade: fidefignidade e totalidade da informação de acordo com valores de negócio e expectativas
  - Disponibilidade: disponibilidade da informação quando exigida pelo processo de negócio hoje e no futuro
  - Conformidade: aderência a leis, regulamentos e obrigações ao quais os processos de negócio estão sujeitos
  - Confiabilidade: entrega de informação apropriada para os executivos administrarem a organização

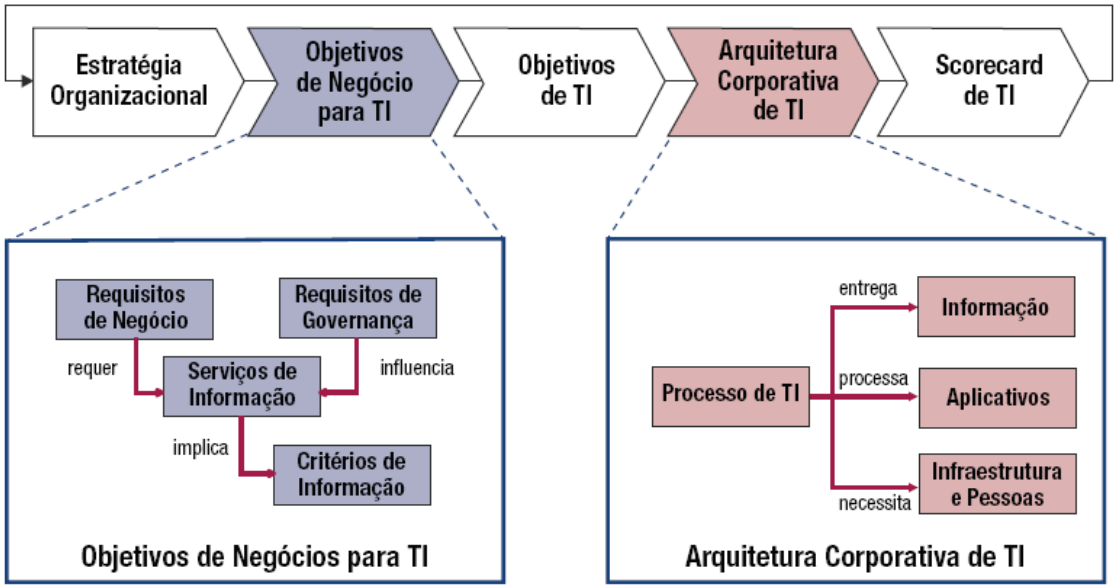
CobiT – Foco em negócios

- Objetivos de negócios e objetivos de TI
  - Uma vez definidos **os objetivos de negócios**, precisamos "*traduzir*" esses objetivos em **objetivos de TI**, de forma a entregarmos um serviço que dê suporte ao processo de negócio.
  - Exemplo:
    - Objetivo de negócio:
      - Vendas via Internet devem ser viabilizar a captação de mais clientes
    - Objetivos de TI:
      - Melhorias na implementação do site da empresa;
      - Compra de novos servidores para suportar novos acessos ao site;
      - Etc...

CobiT – Foco em negócios

- Objetivos de negócios e objetivos de TI

Figura 6 - Definindo os objetivos de TI e a Arquitetura da Empresa para TI



CobiT – Orientação a processos

- O CobiT define as atividades de TI em um modelo de processos com quatro domínios:

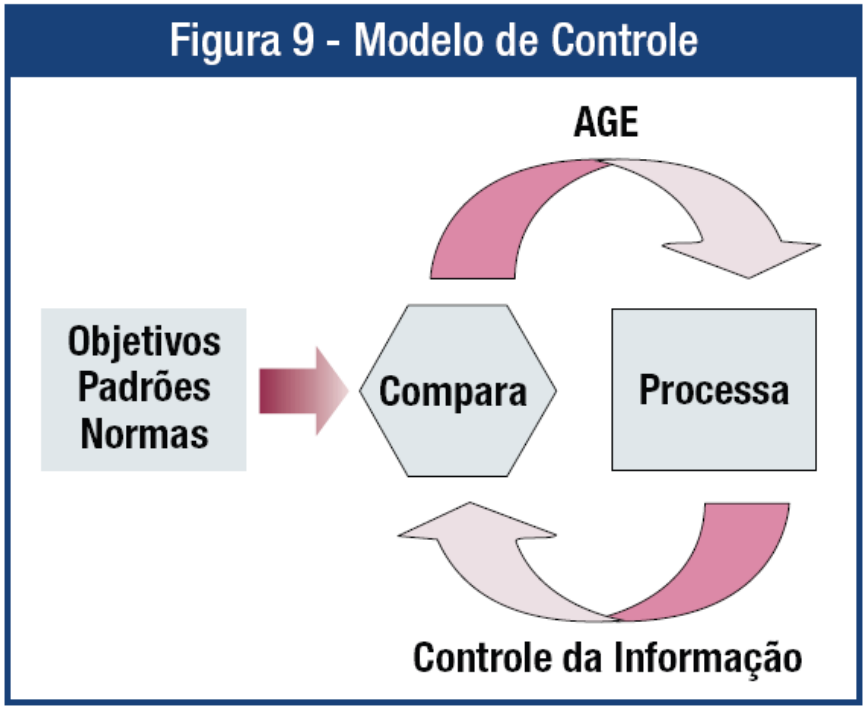
CobiT – Orientação a processos

- Domínios de processo:
  - **Planejar e Organizar**: provê direção para entrega de soluções e entrega de serviços;
  - **Adquirir e Implementar**: provê as soluções e as transfere para tornarem-se serviços
  - **Entregar e Suportar**: recebe as soluções e as torna passíveis de uso pelos usuários finais
  - **Monitorar e Avaliar**: monitora todos os processos para garantir que a direção definida seja seguida

CobiT – Base em controles

- **Controle**: políticas, procedimentos e estruturas organizacionais criadas para garantir que os objetivos de negócio serão atingidos.

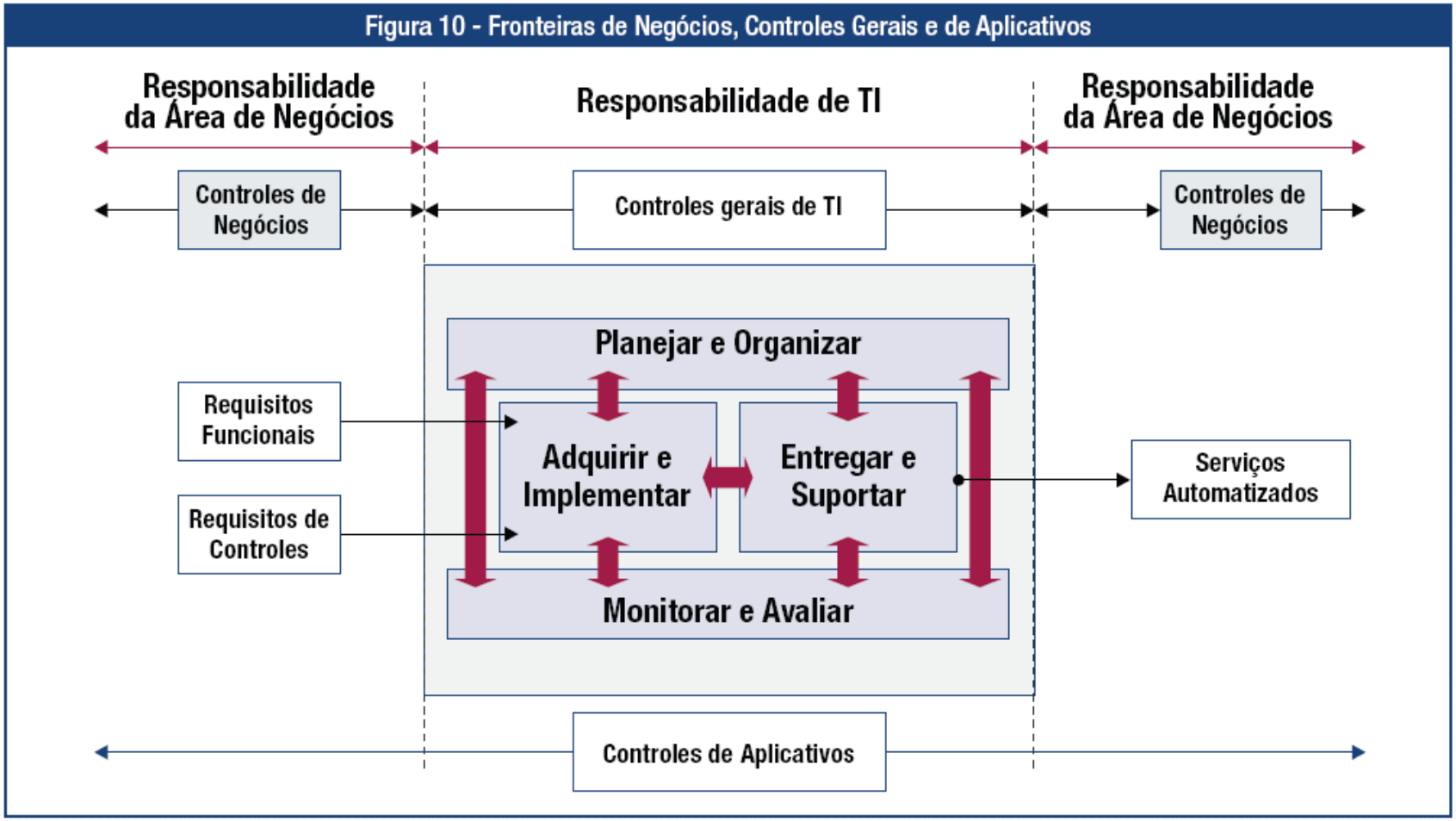
- Com os **objetivos de controle** orientamos os processos de TI a atingirem seus objetivos de uma maneira eficaz.



CobiT – Base em controles

- Cada processo do CobiT tem os seus objetivos de controle, dividido em:
  - **Controles de Negócios:** mediam os processos de negócio, podendo estar integrados aos aplicativos de TI (como um controle de fluxo de caixa, onde o usuário é informado via email sobre determinado evento), ou ser um controle manual (como uma aprovação de um gestor para o processo ir para a próxima etapa).
  - **Controles Gerais de TI:** mediam os processos da área de TI para a execução das tarefas, como a gestão do desenvolvimento de sistemas, do gerenciamento de mudanças, a segurança da infraestrutura, etc.
  - **Controles de Aplicativos:** mediam o controle automatizado dos aplicativos, de como eles lidam com as informações segundo os critérios de informação definidos junto as áreas de negócio.

CobiT – Base em controles



CobiT – Orientação por medições

- Necessidade básica para toda organização: entender qual é a situação atual dos seus próprios sistemas de TI.
- "Quão distantes devemos ir e será que o custo é justificado pelo benefício?"
  - **Não é fácil saber essa resposta.**

CobiT – Orientação por medições

- As organizações precisam saber em que ponto elas estão e onde precisam melhorar (como atingir esse objetivo).
- O CobiT oferece:
  - Modelos de maturidade;
  - Objetivos de performance e métricas para os processos de TI (mensuração através do *Balanced Scorecard*).

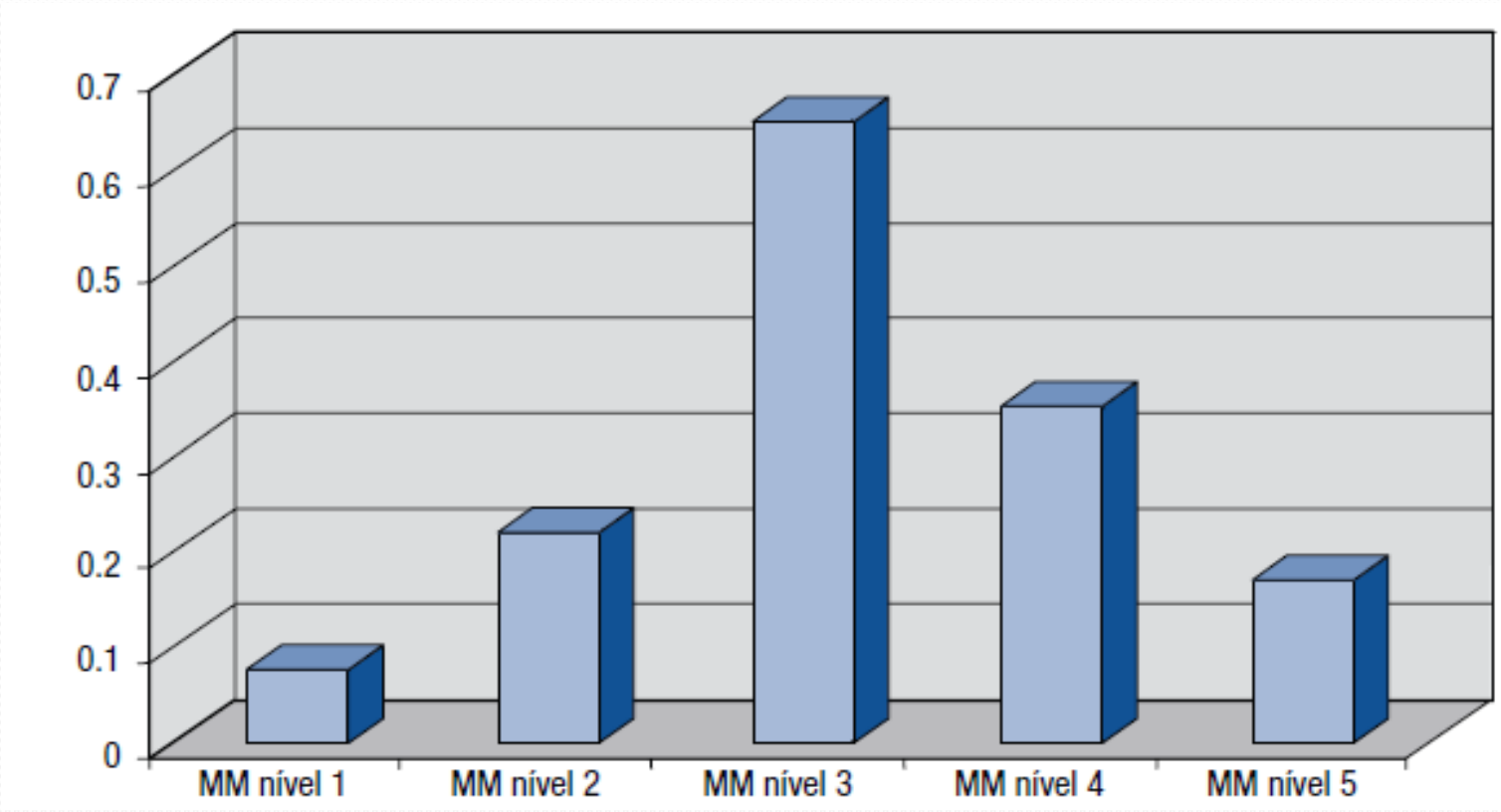
CobiT – Modelos de Maturidade

- Paradigma: “Onde estamos? Para onde vamos? Como progredimos em relação às metas?”
  - Modelo de maturidade para o gerenciamento e controle dos processos de TI, método para avaliar uma organização.
  - O nível de maturidade pode ir de 0 (não-existente) a 5 (otimizado).

CobiT – Modelos de Maturidade

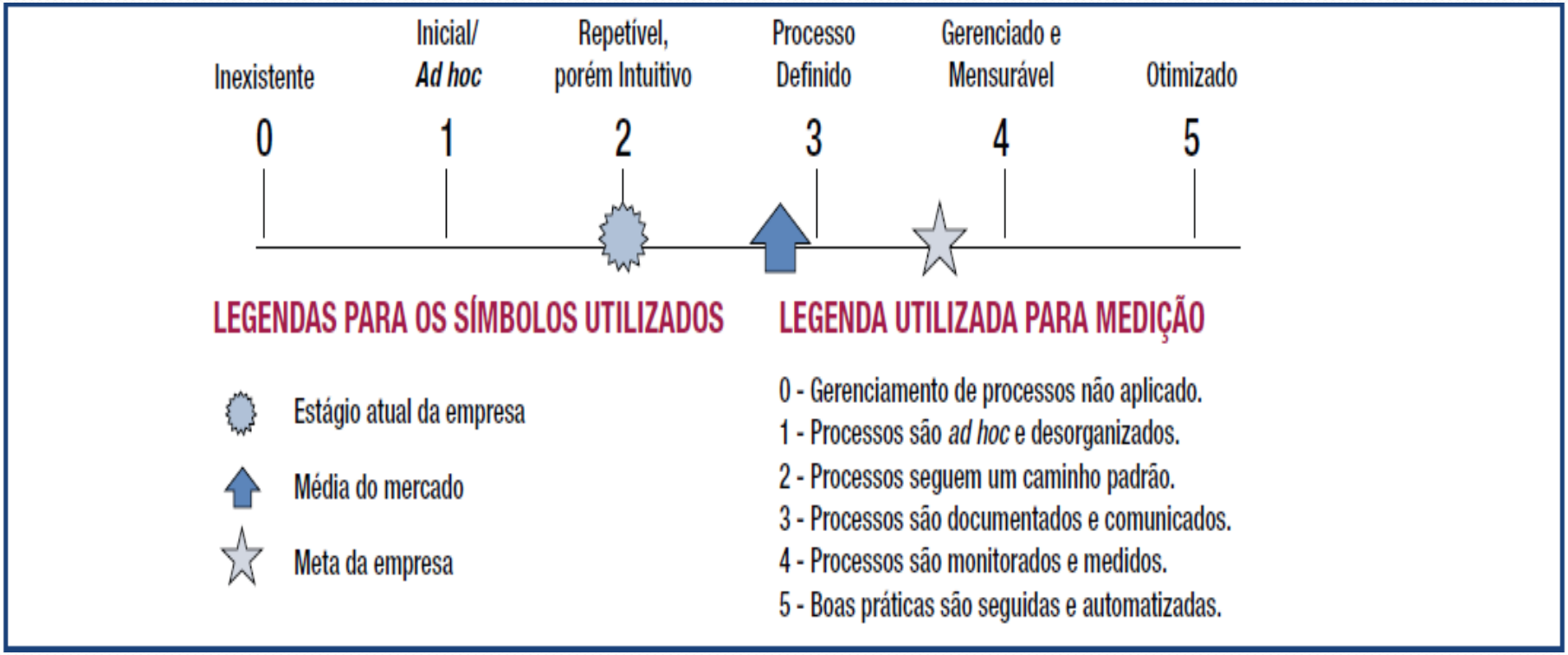
- Enfoque derivado do modelo de maturidade do SEI (Software Engineering Institute), para Engenharia de Software, embora difira consideravelmente do mesmo;
- O modelo proposto pelo CobiT não tem o intuito de certificar que um determinado nível foi atingido.

CobiT – Modelos de Maturidade



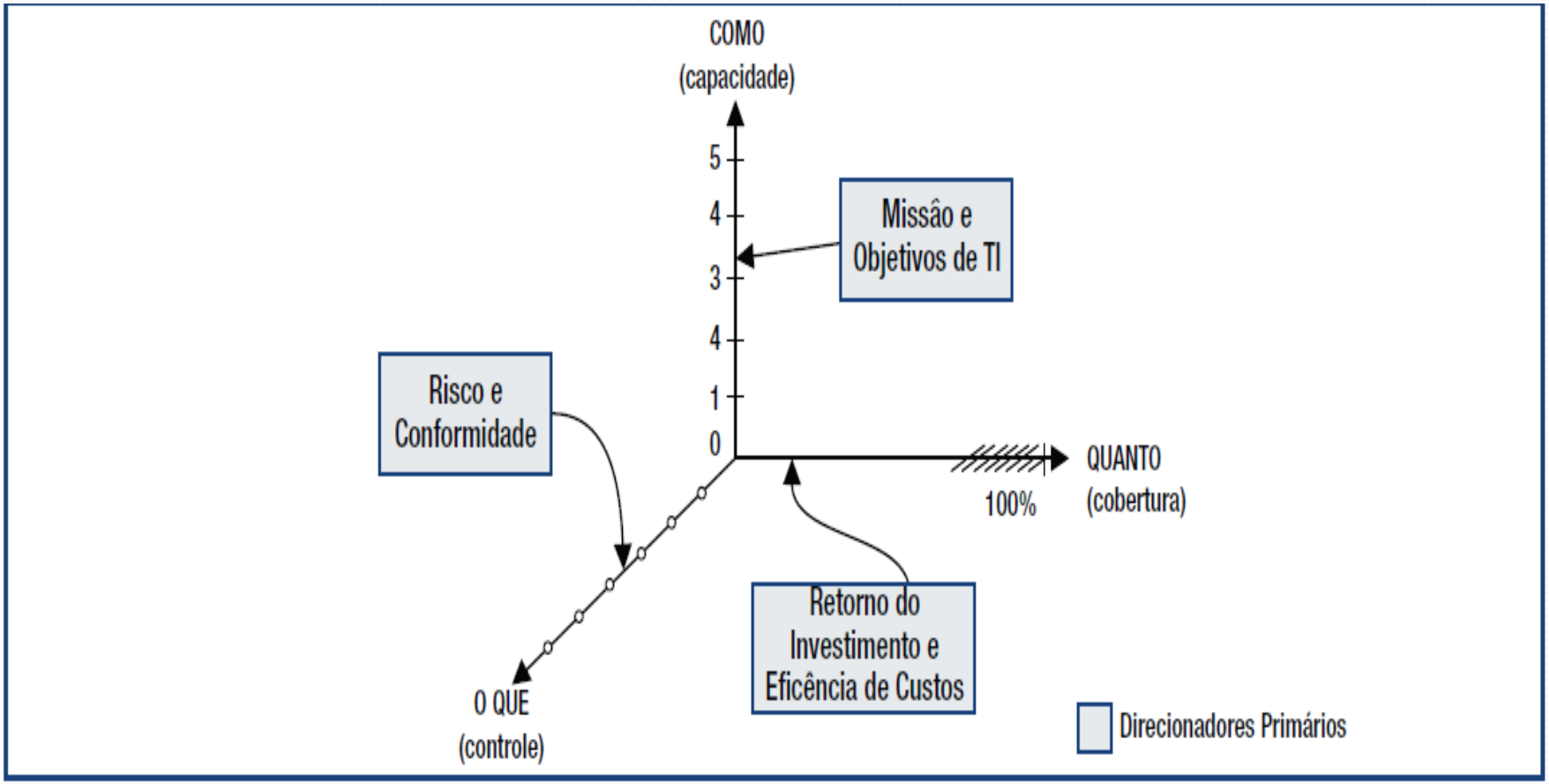
Possível nível de maturidade de um processo de TI: uma implementação pode estar em andamento em diferentes níveis de maturidade, mesmo que não de maneira completa.

CobiT – Modelos de Maturidade



<u>Escala de Maturidade:</u> aplicada a cada um dos 34 processos de TI do CobiT, a gerência pode ter respostas para o "Onde estamos? Para onde vamos? Como progredimos em relação às metas?".

CobiT – Modelos de Maturidade



As três dimensões da maturidade: capacidade, cobertura e controle (um ambiente corretamente configurado deve considerar esses aspectos).

CobiT – Modelos de Maturidade

- Atributos adicionados de maneira crescente através dos níveis de maturidade:
  - Consciência e comunicação;
  - Políticas, planos e procedimentos;
  - Ferramentas e automação;
  - Habilidades e especialização;
  - Responsabilidade e responsabilização;
  - Definição de objetivos e medição.

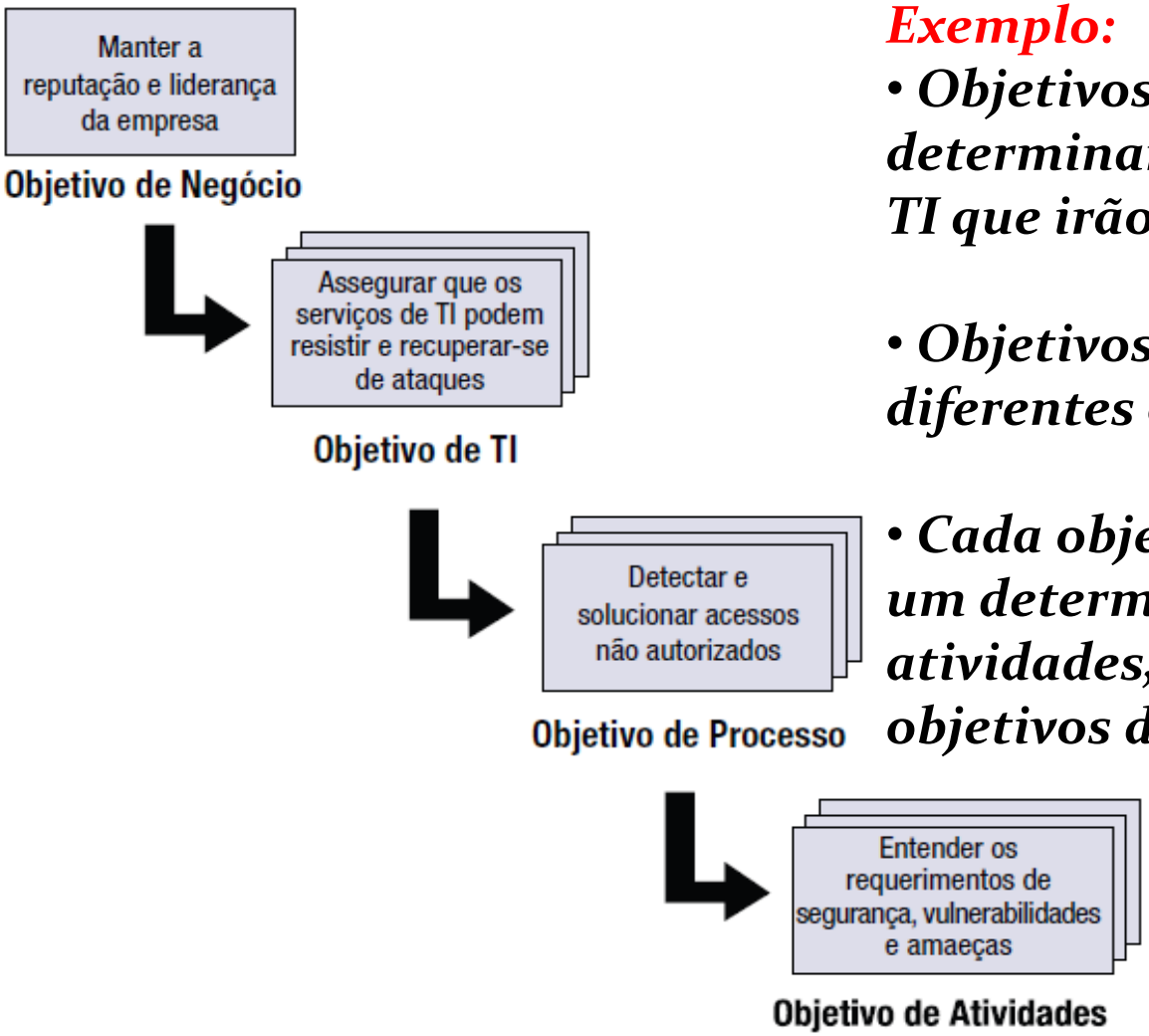
CobiT – Modelos de Maturidade

- A melhora da maturidade de um processo significa:
  - Redução de custos;
  - Maior eficiência;
  - Processos mais previsíveis;
  - Uso eficiente dos recursos.

CobiT – Medição de Performance

- Objetivos e métricas definidos em três níveis:
  - Em TI, representando o que os negócios esperam de TI e como medir isso;
  - Em processos, representando o que os processos de TI precisam entregar para suportar os objetivos de TI e como medir isso;
  - Em atividades, para estabelecer o que precisa ser feito dentro do processo para atingir a performance requirida e como medir isso.

CobiT – Medição de Performance



Exemplo:

- ***Objetivos de negócios determinam os vários objetivos de TI que irão suportá-los.***

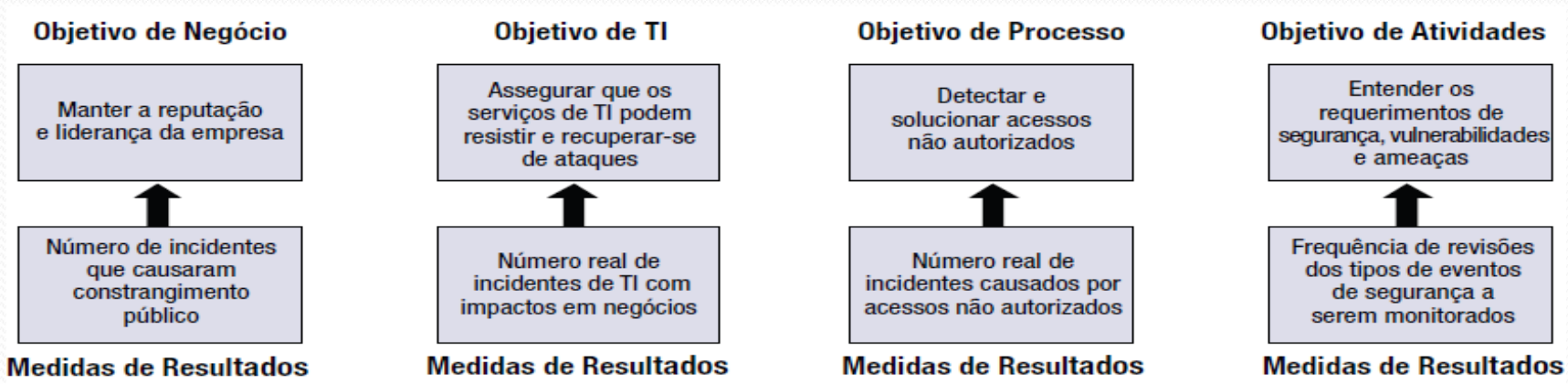
- ***Objetivos de TI influenciam diferentes objetivos de processos.***

- ***Cada objetivo de processo exige um determinado número de atividades, estabelecendo os objetivos da atividade.***

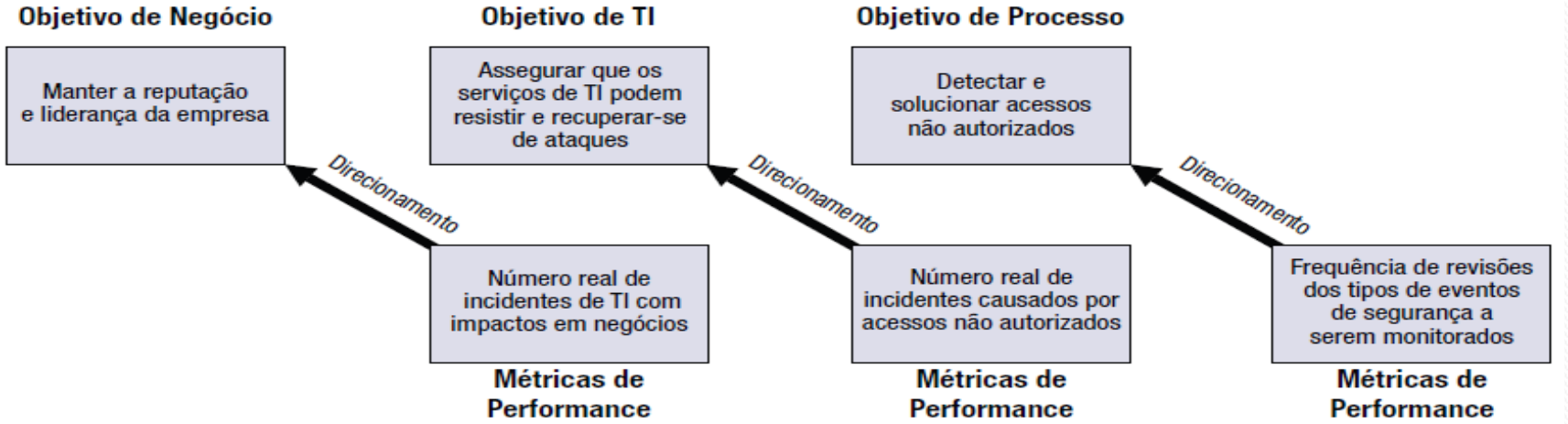
CobiT – Medição de Performance

VERSÕES ANTERIORES DO COBIT	COBIT 4.1	DESCRIÇÃO
KGIs (Indicadores-chaves de objetivos).	**Medidas de resultados (saídas).**	Indicam se os objetivos **FORAM** atingidos; indicadores históricos.
KPIs (Indicadores-chaves de performance).	**Indicadores de performance.**	Indicam se os objetivos **SERÃO** atingidos; indicadores futuros.

CobiT – Medição de Performance



As medidas de resultados no menor nível se tornam indicadores de performance para o nível acima.

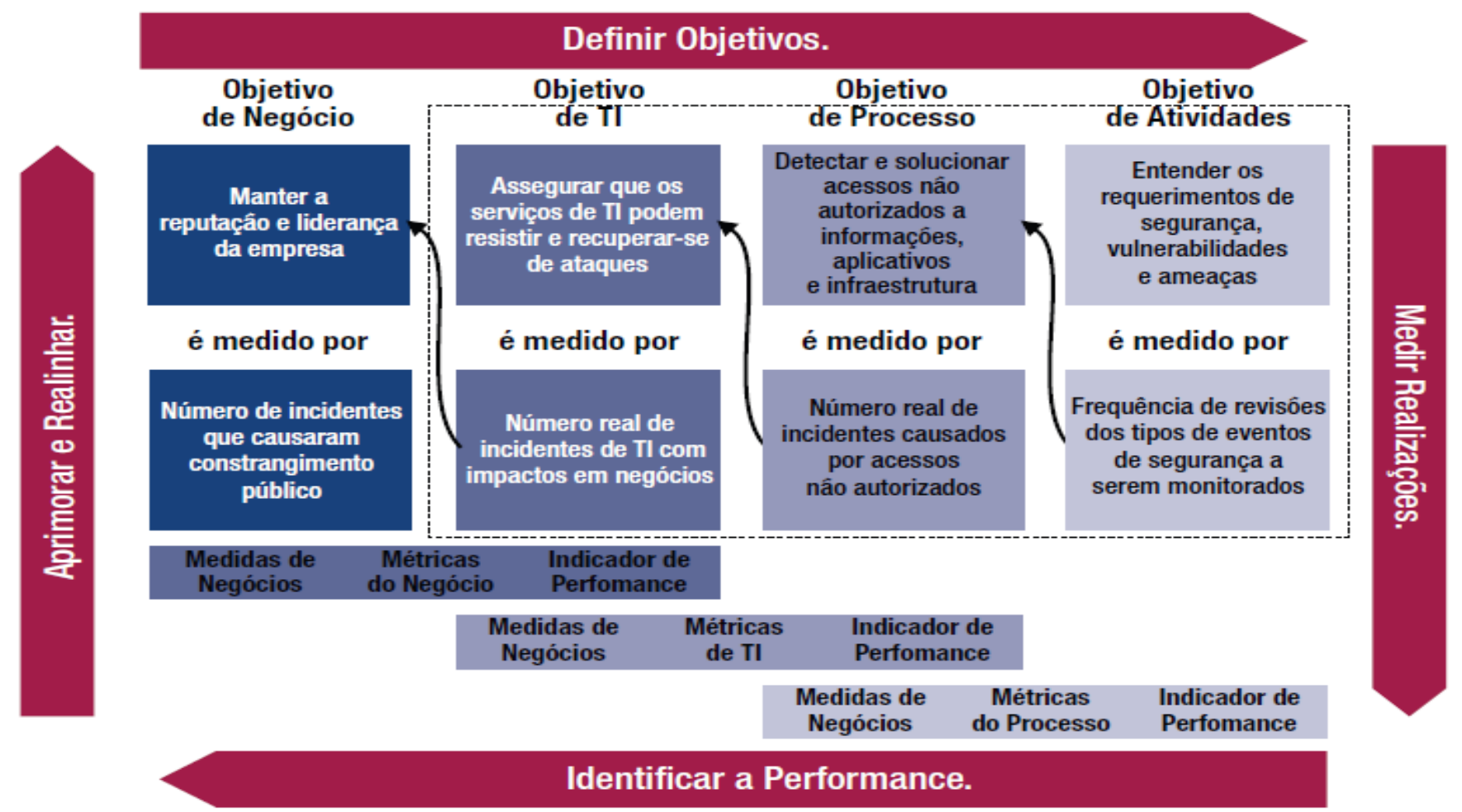


CobiT – Medição de Performance

- Os medidores de resultados de TI às vezes são expressos em termos de:
  - Disponibilidade da informação requerida para suportar as necessidades de negócios;
  - Ausência de riscos de integridade e confidencialidade;
  - Eficiência de custos de processos e operação;
  - Confirmação de fidedignidade, efetividade e conformidade.

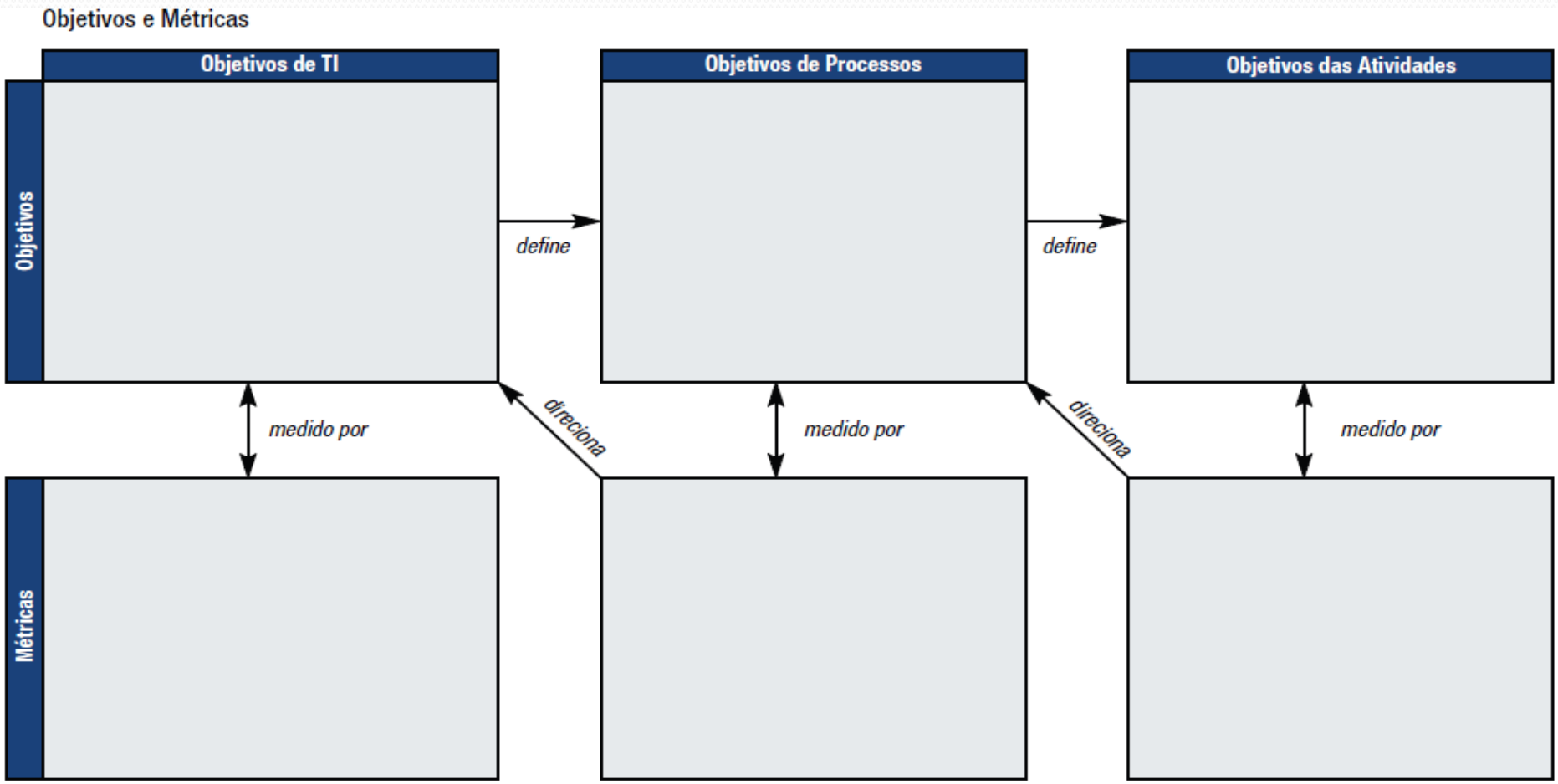
- Visões distintas: um ***serviço*** entregue por TI é **um objetivo para TI**. Porém, **para negócios**, esse serviço é **um indicador de performance e capacidade**.

CobiT – Medição de Performance



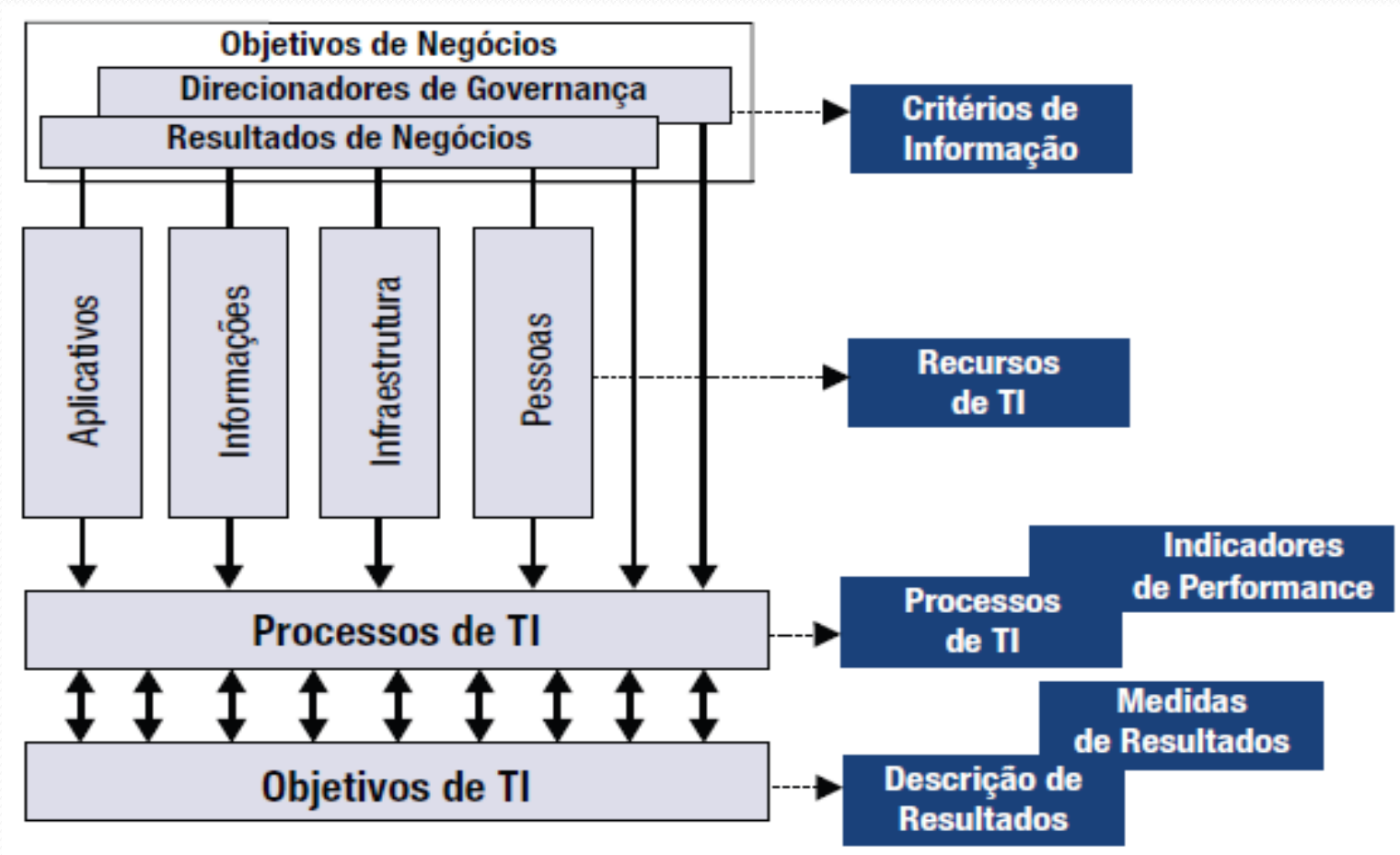
Relacionamento entre processos, objetivos e métricas.

CobiT – Medição de Performance



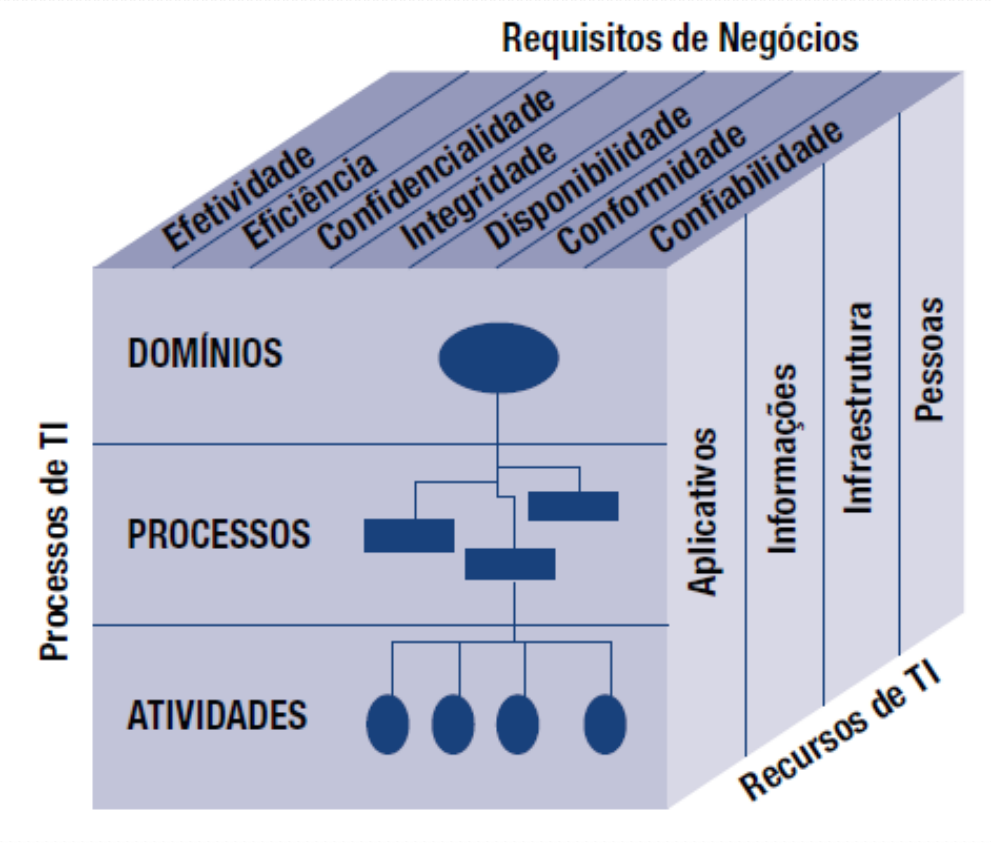
Apresentação dos objetivos e métricas para cada processo de TI no CobiT (fácil para mensurar sem confundir com metas).

CobiT – Estrutura do modelo



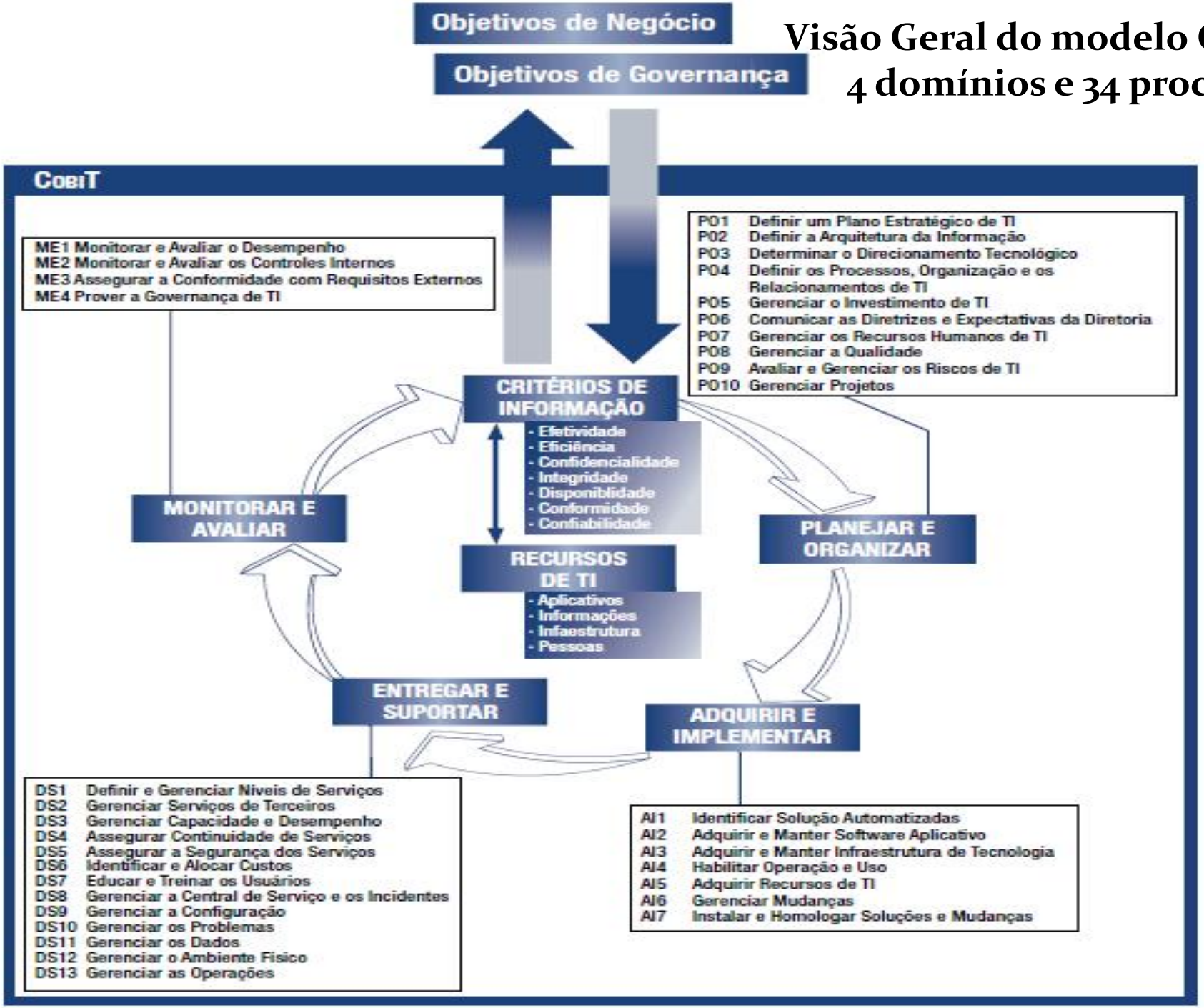
Gerenciamento, Controle, Alinhamento e Monitoramento do CobiT.

CobiT – Estrutura do modelo



Princípio básico do modelo CobiT: os recursos de TI são gerenciados pelos processos de TI para atingir os objetivos de TI que correspondem aos requisitos de negócios.

Visão Geral do modelo CobiT: 4 domínios e 34 processos.



CobiT – Aceitabilidade Geral

- Recomendável a utilização em um alto nível, para prover uma metodologia geral com base em um modelo de processos de TI que deve servir genericamente para toda empresa.

- O CobiT foi desenhado para ser complementar e utilizado com outros padrões e boas práticas (ITIL, CMM, ISSO 17799, PMBOK).

CobiT – Aceitabilidade Geral

- A implementação de boas práticas deve ser consistente com a governança e o ambiente de controle da organização;

- A gerência e os funcionários devem entender o que fazer, como fazer e porque isso é importante.

CobiT – Aceitabilidade Geral

- Diferentes usuários são influenciados:
  - Alta direção;
  - Executivos de negócios;
  - Executivos de TI;
  - Auditores.
- O CobiT foi desenvolvido e é mantido por um instituto de pesquisa independente e sem fins lucrativos; seu conteúdo baseia-se em contínua pesquisa.

CobiT – Aceitabilidade Geral

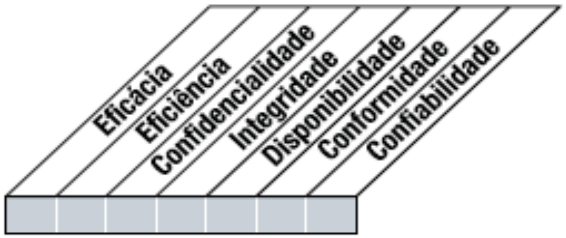
	Objetivos	Métricas	Práticas	Modelos de Maturidade
Alinhamento Estratégico	P	P		
Entrega de Valor		P	S	P
Gerenciamento de Risco		S	P	S
Gerenciamento de Recursos		S	P	P
Gerenciamento de Performance	P	P		S

P = Ferramenta Primária S = Ferramenta Secundária

Modelo CobiT e as áreas foco da governança de TI (o CobiT é orientado para os objetivos e escopo da governança de TI).

CobiT – Descrição dos processos

- **1ª seção** para cada processo do CobiT:
  - Contém uma descrição do processo, que resume os objetivos do mesmo, apresentada no formado de cascata
  - Demonstra o mapeamento dos critérios (a letra P indica um relacionamento primário e a letra S um relacionamento secundário).



Controle sobre o seguinte processo de TI:

Nome do processo

que satisfaça aos seguintes requisitos do negócio para a TI:

sumário do objetivo de TI mais importante

com foco em:

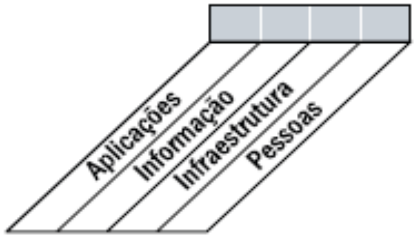
sumário dos objetivos de processos mais importantes

é alcançado por:

objetivos da atividade

e medido por:

métricas chaves



Exemplo da 1ª seção de um processo no CobiT.

CobiT – Descrição dos processos

- **2ª seção** apresenta os objetivos de controle do processo.
- **3ª seção:**
  - Processos de entrada e saída;
  - Tabela RACI (distribuindo responsabilidades para o CEO, CFO, Executivo de Negócio, CIO, ...);
  - Objetivos e métricas.
- **4ª seção** apresenta o modelo de maturidade do processo.

CobiT – Descrição dos processos

- Outro modo de visualizar a performance do processo é avaliar se:
  - As entradas do processo são as esperadas;
  - A descrição dos objetivos de controle do processo define o que deve ser feito;
  - As saídas do processo são aquelas que realmente devem ser entregues;

CobiT – Descrição dos processos

- Os objetivos e métricas demonstram como o processo deve ser medido;
- A tabela RACI define o que precisa ser delegado e para quem;
- O modelo de maturidade demonstra o que precisa ser feito para o aprimoramento.

Domínios do CobiT

- Planejar e Organizar
- Adquirir e Implementar
- Entregar e Suportar
- **Monitorar e Avaliar**

Domínio Monitorar e Avaliar

- ME1 Monitorar e Avaliar o Desempenho de TI
- ME2 Monitorar e Avaliar os Controles Internos
- ME3 Assegurar a Conformidade com Requisitos Externos
- ME4 Prover Governança de TI

ME1 Monitorar e Avaliar o Desempenho de TI

- Transparência e entendimento de custos
- Benefícios
- Estratégia
- Políticas e Níveis de serviço de TI

ME1 Monitorar e Avaliar o Desempenho de TI

- ME1.1 Abordagem de Monitoramento
  - Estrutura de monitoramento geral
- ME1.2 Definição e Coleta dos Dados de Monitoramento
  - Definir comparativos (Benchmarks)
- ME1.3 Método de Monitoramento
  - Apresentar um visão ampla do desempenho da TI

ME1 Monitorar e Avaliar o Desempenho de TI

- ME1.4 Avaliação de Desempenho
  - Analisar o desempenho com base nas metas
- ME1.5 Relatórios para a Alta Direção
  - Desenvolver informes sobre a contribuição da TI
- ME1.6 Ações Corretivas
  - Baseadas no monitoramento, avaliação e relatórios de desempenho

ME1 Monitorar e Avaliar o Desempenho de TI

- **0** Inexistente
  - Processo de monitoramento não implementado
- **1** Inicial
  - Reconhecimento da necessidade de coletar informações sobre o processo de monitoramento
- **2** Repetível
  - Identificação das métricas a serem monitoradas

ME1 Monitorar e Avaliar o Desempenho de TI

- **3** Processo Definido
  - Oficialização dos processos padrão de monitoramento
- **4** Gerenciado e Mensurável
  - Definição das regras sobre as quais o processo deve operar
- **5** Otimizado
  - Incorporar melhores práticas

ME2 Monitorar e Avaliar os Controles Internos

- Assegurar que os objetivos de TI sejam atingidos
- Assegurar a conformidade comas leis e os regulamentos relacionados à TI

ME2 Monitorar e Avaliar os Controles Internos

- ME2.1 Monitoramento da estrutura de Controles Internos
  - Monitorar o ambiente e a estrutura de TI
- ME2.2 Revisão Gerencial
  - Eficiência e Eficácia das revisões gerenciais
- ME2.3 Exceções aos Controles
  - Análise Crítica das Causas-Raiz
- ME2.4 Auto Avaliação dos Controles
  - Grau de Abrangência e efetividade dos controles internos

ME2 Monitorar e Avaliar os Controles Internos

- ME2.5 Garantia dos Controles Internos
  - Avaliações de terceiros
- ME2.6 Controles Internos Aplicados a Terceiros
  - Certificar-se de que fornecedores externos cumpram suas obrigações
- ME2.7 Ações Corretivas
  - Baseadas nas avaliações e nos relatórios de controle

ME2 Monitorar e Avaliar os Controles Internos

- **0** Inexistente
  - Sem procedimentos a eficácia dos controles internos
- **1** Inicial
  - Reconhecimento da necessidade e gerenciamento de TI
- **2** Repetível
  - Uso de relatórios informais

ME2 Monitorar e Avaliar os Controles Internos

- **3** Processo Definido
  - Apoio e institucionalização dos controles internos
- **4** Gerenciado e Mensurável
  - Implementação de estrutura para monitoramento dos controles internos
- **5** Otimizável
  - Programa corporativo de melhoria contínua

ME3 Assegurar a Conformidade com Requisitos Externos

- ME3.1 Identificação Requisitos de conformidade com leis, regulamentações e contratos externos
  - Identificar continuamente exigências de leis, regulamentos e contratos locais e internacionais que devem ser atendidos.

- ME3.2 Otimização da resposta aos requisitos externos
  - Revisar e ajustar políticas, padrões, procedimentos e metodologias de TI para garantir o atendimento e comunicação dos requisitos legais e regulatórios.

ME3 Assegurar a Conformidade com Requisitos Externos

- ME3.3 Avaliação da conformidade com requisitos externos
  - Confirmar a conformidade de políticas, padrões, procedimentos e metodologias de TI com os requisitos legais e regulatórios.

- ME3.4 Assegurar a conformidade
  - Confirmar tomada de ações corretivas de maneira oportuna para resolver qualquer desvio no cumprimento das conformidades.

- ME3.5 Informes Integrados
  - Integração de informes de TI sobre requisitos legais, regulatórios e contratuais a informes similares pertencentes a outras funções do negócio.

ME3 Assegurar a Conformidade com Requisitos Externos

- **O gerenciamento do processo pode ser:**

- **0** Inexistente
  - Pouca consistência sobre requisitos externos.

- **1** Inicial / Ad hoc
  - Há consistência.
  - São adotados processos informais para manter a conformidade, porém apenas quando há necessidade em novos projetos, reposta a auditorias ou análises críticas.

ME3 Assegurar a Conformidade com Requisitos Externos

- **2** Repetível, porém indutivo
  - Entendimento da necessidade de adesão.
  - Não há abordagem padronizada: probabilidade de erros.

- **3** Processo Definido
  - Foram desenvolvidos e documentados processos.
  - Existência de treinamentos sobre requisitos.
  - Nem sempre podem ser cumpridos integralmente e podem estar desatualizados ou ser inviáveis.
  - Pouco monitoramento.

ME3 Assegurar a Conformidade com Requisitos Externos

- **4** Gerenciado e Mensurável
  - Completo entendimento da necessidade de assegurar a conformidade.
  - Esquema de treinamento formal.
  - Revisão do ambiente para identificar requisitos externos e mudanças constantes.

- **5** Otimizado
  - Processo bem organizado, eficaz e obrigatório.
  - Função central e única que fornece coordenação para toda a organização.
  - Vasto conhecimento dos requisitos externos aplicáveis, tendências futuras e mudanças previstas.

ME4 Prover Governança de TI

- ME4.1 Estabelecimento de uma estrutura de governança de TI
  - Definição, estabelecimento e alinhamento da estrutura de governança de TI com a governança organizacional e o ambiente de controle.
  - Estruturar conforme processos e modelos adequados e implementar práticas e responsabilidades claras para evitar falhas de controle interno e supervisão.
  - Geração de relatórios sobre status da governança de TI e questões relacionadas.

ME4 Prover Governança de TI

- ME4.2 Alinhamento estratégico
  - A alta direção deve ser habilitada no entendimento das questões estratégicas de TI.
  - Certificar-se de que há entendimento compartilhado entre o negócio e a TI.
  - Comitê de estratégia de TI, trabalhando com conselho do diretor, definindo e implementando.

ME4 Prover Governança de TI

- ME4.3 Entrega de Valor
  - Gerenciamento dos investimentos para assegurar maior valor possível no suporte aos objetivos e estratégia do negócio.
  - Abordagem disciplinada de gerenciamento de portfólio, programas e projetos.
  - Responsabilidades sobre investimento de TI.

ME4 Prover Governança de TI

- ME4.4 Gerenciamento de Recursos
  - Supervisão de investimentos, uso e alocação de recursos de TI.
  - Avaliações periódicas visando assegurar a suficiência de recursos.

- ME4.5 Gestão de Riscos
  - Definir o apetite corporativo em conformidade com o diretor, obtendo assim segurança sobre a adequação das práticas de gerenciamento de TI.
  - Assegurar que os riscos de TI não excedem o apetite de risco da alta direção.

ME4 Prover Governança de TI

- ME4.6 Medição de Desempenho
  - Confirmar os objetivos acordados de TI para verificar se foram atingidos ou excedidos e se seu progresso atende às expectativas.
  - Reportar para a Alta Direção os portfólios, programas e desempenho de TI relevantes.

- ME4.7 Avaliação Independente
  - Obter avaliação sobre a conformidade de TI com leis e regulamentos relevantes, políticas, padrões e procedimentos organizacionais.

ME4 Prover Governança de TI

- **Gerenciamento do processo:**

- **0** Inexistente
  - Não existe processo identificável de governança de TI, nem comunicação sobre o assunto.

- **1** Inicial / Ad Hoc
  - Há reconhecimento sobre a necessidade, a direção tem apenas uma informação aproximada sobre o assunto.
  - Só existem comunicações inconsistente e esporádicas sobre as questões.

ME4 Prover Governança de TI

- **2** Repetível, porém indutivo
  - Há conscientização das questões de governança de TI.
  - A diretoria tem conhecimento de técnicas de avaliação e medição, mas não tem sido adotado na organização.
  - Pouca experiência com as funcionalidades.

- **3** Processo Definido
  - É compreendida a importância da governança de TI.
  - É estabelecido treinamento.
  - Há monitoramento, porém podem existir desvios não detectados pela direção.

ME4 Prover Governança de TI

- **4** Gerenciado e Mensurável
  - Completo entendimento em todos os níveis.
  - Responsabilidades claras e propriedade dos processos estabelecida.
  - Integração e alinhamento dos processos e da governança de TI.
  - Definição de tolerâncias sob as quais os processos devem operar.
  - Monitoramento de indicadores de desempenho, gerando aprimoramentos para toda a empresa.

ME4 Prover Governança de TI

- **5** Otimizado
  - Entendimento avançado apontando para o futuro.
  - São utilizadas formas mais avançadas para treinamento e comunicação.
  - Qualquer problema ou desvio tem sua causa-raiz analisada, e são identificadas e tomadas ações eficientes de maneira sistemática.
  - As atividades de governança de TI são integradas ao processo de governança corporativa.

Referências

- **IT GOVERNANCE INSTITUTE (ITGI)**. CobiT® framework. Ilinois: IT Governance Institute, 2007.

- TERZIAN, Françoise. **Todo poder ao Cobit.** Info CORPORATE, 2008. Disponível em: <http://info.abril.com.br/corporate/aplicacoes-de-gestao/todo-poder-ao-cobit.shtml>. Acesso em: 17 mai. 2010.